*****PUBLIC VERSION*****

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 The Honorable Judge Ellis Hearing: Sept. 11, 2020

MR. ZACKARY ELLIS SANDERS'S REPLY TO THE GOVERNMENT'S OMNIBUS OPPOSITION TO MR. SANDERS'S MOTIONS TO SUPPRESS

Zackary Ellis Sanders, by and through undersigned counsel, respectfully submits this Reply to the Government's Omnibus Opposition to Mr. Sanders's Motions to Suppress.

INTRODUCTION

This Court is presented with two issues that are both dispositive in Mr. Sanders's favor:

- *Lack of a Substantial Basis for Probable Cause*. When an affidavit depends on an informant's conclusory tip—even from a foreign law enforcement officer—whether a Magistrate Judge can credit that hearsay depends on the tip's corroboration through other sources. No Court has ever found a substantial basis for probable cause from a single, uncorroborated tip when [redacted]; the FBI took no steps to—and did not—corroborate it in any manner. The question Mr. Sanders's Motion to Suppress No. 1 presents is: Should

this Court break new legal ground by finding substantial grounds for probable cause on the sole basis of an exceedingly vague and entirely uncorroborated tip?

- *Materially Misleading Statements and Omissions*. When the FBI applies for a search warrant, it cannot knowingly or recklessly mislead a Magistrate with an affidavit that hinges on deceptive statements or omissions. If the FBI does so, an accused is entitled to a *Franks* hearing. Here, the Special Agent knowingly and recklessly misled the Magistrate by [redacted].[1]

  The question Mr. Sanders's Motions to Suppress Nos. 2-4 presents is: Should this Court deny Mr. Sanders a *Franks* hearing where he has made a substantial evidentiary showing that the Special Agent materially misled the Magistrate?

The answer to both of the questions presented must be no. That is particularly true with respect to the search of a family's home, including all electronic devices within it. Such sensitive areas are especially deserving of strict Fourth Amendment protection.[2]

Even if the Affidavit was not materially misleading—which it was—this Court would have to break new ground to affirm probable cause. There are no cases—not just in this District

[1] *See* Affidavit, attached to Motion to Suppress No. 1 (ECF No. 81), as Ex. 1, and referred to throughout this motion as "Affidavit."

[2] *See, e.g. Riley v. California*, 134 S. Ct. 2473, 2490-91 (2014) (requiring strict adherence because electronically-stored data can reveal a person's most private thoughts and interests and "would typically expose the government to far more than the most exhaustive search of a house").

or Circuit, but anywhere in the United States—finding probable cause based only on an uncorroborated, vague, and conclusory tip of this nature, even one from a foreign law enforcement officer. Nor, in the context of child pornography investigations, are there any cases finding probable cause based only on a [redacted],[3] without any facts to show that [redacted]. In the cases the Government attempts to take refuge in throughout its Opposition, the courts have consistently required significantly more than what the FBI had here.

In addition, had the Special Agent disclosed what he knew about the lack of evidence, the Magistrate would not have had a substantial basis to believe that this Internet user did anything illegal or that evidence of wrongdoing could be found in the Sanders's family home. With sworn declarations from four defense experts, Mr. Sanders has shown that the Special Agent knowingly (or, at a minimum, recklessly) misled the Magistrate into drawing the incorrect inferences necessary to finding probable cause. The good faith exception accordingly does not apply. All evidence derived from the search of the Sanders's family home must be suppressed.

ARGUMENT

I. An uncorroborated, vague and conclusory tip does not provide a Magistrate with a substantial basis for finding probable cause: without corroboration of the foreign officer's hearsay, the conclusion that this Internet user ever actually viewed—or intended to view—illegal content was not reasonable.

To provide a Magistrate with the required "substantial basis for determining the existence of probable cause," an affidavit that relies on an informant's tip requires "corroboration through

[3] Contrary to what the Government has said repeatedly, including most recently throughout its Opposition, it is not true that [redacted] Opp'n at 3, 4, 8, 12, 19-20, 26-28. [redacted]

other sources of information" that "reduce[] the chances of a reckless or prevaricating tale."[4] An officer can rely on an informant's hearsay only "so long as the informant's statement is reasonably corroborated by other matters within the officer's knowledge."[5] "Mere affirmance of belief or suspicion [of another] is not enough."[6]

The Affidavit in this case depended entirely on the uncorroborated, vague tip from a foreign officer that [redacted] Affidavit, ¶ 23. Despite being 36 pages and 54 paragraphs long, only one paragraph—Paragraph 23—alleged that [redacted][8] Affidavit, ¶ 23. Yet, the Affidavit did not allege that [redacted]

[4] *Illinois v. Gates*, 462 U.S. 213, 239, 244-45 (1983).

[5] *Jones v. United States*, 362 U.S. 257, 269 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83 (1980).

[6] *Nathanson v. United States*, 290 U.S. 41, 47 (1933).

[7] The [redacted] FD-1057, attached to Motion to Suppress No. 1 (ECF No. 81) as Ex. 4. The Special Agent omitted this information from the Affidavit.

[8] Contrary to what the Affidavit strongly suggested, [redacted]

[redacted].[9]

The remainder of the Affidavit consisted of 53 other paragraphs that show the FBI did not corroborate Paragraph 23. Six paragraphs simply [redacted]. The remaining 47 paragraphs consisted of [redacted]. None of these 47 paragraphs provide facts specific to the Internet user nor do they corroborate the Internet user's purported activity on [redacted].

The Government misses the mark in asserting that tips from law enforcement are universally—and without more—sufficient for probable cause.[10] The Government's quotation

[9] *See, e.g.*, Order Granting the Defendant's Motion to Suppress in *United States v. Larry James Reece, II*, 16-CR-104 (E.D. Va. 2017) ("*Reece* Order"), attached to Mr. Sanders's Notice of Filing (Sept. 9, 2020) (ECF No. 93) as Ex. A, at 11, 13.

[10] For example, the Third Circuit ruling, in *United States v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013) that *on the high seas*, the U.S. Coast Guard can rely on a tip from a foreign law enforcement agency for reasonable suspicion—not probable cause—to stop *briefly* and board a vessel pursuant to an international agreement to prevent drug trafficking is inapplicable here. It does not follow that a sweeping search of a family's home and devices, conducted on U.S. soil, pursuant to a warrant, can be justified on the basis of a vague and conclusory tip—even one from a foreign law enforcement officer.

from *United States v. Hodge*, 354 F.3d 305, 307-09 (4th Cir. 2004), is unpersuasive.[11] To be clear, Mr. Sanders does not argue that there needs be a "special showing" of reliability in the case of a law enforcement tip; rather, given the content of the tip and total lack of corroboration, he argues that there needed to be more here, as there was in *Hodge*. In an unpublished Sixth Circuit opinion, *United States v. Hampton*, 504 F. App'x 402, 403 (6th Cir. 2012), the Court held that U.S. law enforcement could rely on a tip from German law enforcement that an individual with a specific IP address offered to and did distribute child pornography, that he had previously joined and subscribed to a child pornography website, that he had remained a subscriber to that website for at least four months,[12] and where German authorities forwarded U.S. officials evidence that the individual "*possessed or distributed* child pornography on three dates between January 2008 through March 2009."[13] The substance of that tip was thus far less vague and stands for the proposition that significantly more specificity was required than what the FBI had here.

As Mr. Sanders made clear in his Motion to Suppress, the tip here was both general and vague and, given its sparseness, required further investigation. The cases the Government cites in opposition do not suggest otherwise and in fact support Mr. Sanders's position. In *United States v. Yusuf*, 461 F.3d 374, 385 (3rd Cir. 2006), the Court found that a tip from a foreign law enforcement agency is not "*per se* reliable," even when obtained pursuant to a court order. Rather, the court noted that "information received from another governmental agency may raise

---

[11] Further, in *Hodge*, the Fourth Circuit upheld a warrant based on information from two undercover detectives who had purchased cocaine from the defendant and an informant who gave very specific details regarding the defendant's narcotics operation. *Id.*

[12] *United States v. Hampton*, 504 F. App'x 402, 403-04 (6th Cir. 2012).

[13] *United States v. Hampton*, No. CRIM.A. 10-39-JBC, 2010 WL 4284953, at *1 (W.D. Ky. Oct. 22, 2010), aff'd, 504 F. App'x 402 (6th Cir. 2012).

questions as to its accuracy and require an agent to undertake further investigation" and held that the defendant would need to show that the information provided "would have put a reasonable official on notice that further investigation was necessary."[14] That is exactly what Mr. Sanders has argued here: that where the tip was this vague and general, "further investigation" of the information—of which there was none—"was necessary" prior to obtaining a warrant to search all of a family's home.[15] That failure was fatal to finding probable cause.

A. No Court has ever found probable cause based on so little evidence.

To find a substantial basis for probable cause, Courts have required more than an uncorroborated, vague, and conclusory tip—even when it comes from law enforcement. Furthermore, "[m]inimal corroboration" of a tip, especially one as conclusory and vague as this one, is insufficient.[18] An informant's tip is insufficient when "the only corroboration [the officer] provided was that the informant's directions to [the defendant]'s home were correct. Almost anyone can give directions to a particular house without knowing anything of substance about what goes on inside that house, and anyone who occasionally watches the evening news can make generalizations about what marijuana looks like and how it is packaged and sold."[19] Here, the FBI was only able to corroborate the innocent fact that the IP address [redacted] was assigned to a computer in the United States; the FBI was unable to corroborate the purported activity of that IP address [redacted].

[14] *Id.*

[15] *Id.*

[18] *United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir. 1996).

[19] *Id.* at 121 (also finding that the good faith exception did not apply).

Generally, a warrant based on an informant's tip must be substantially corroborated.[21] Even in investigative stop cases that require only reasonable suspicion, where the tipster is a law enforcement officer or agency, the corroboration requirement still applies.[22] Thus, courts have always required more than what this Affidavit purported to [redacted],[23] and a vague, imprecise, uncorroborated tip like the one in this case falls well short.

---

[21] *See, e.g., United States v. Reed*, 788 Fed. App'x. 903, 907 (4th Cir. 2019) (upholding warrant based on information provided by concerned citizen because of officers' confirmation: officers confirmed specific address where drugs were allegedly being sold; officers confirmed description of two vehicles; and two controlled buys were recorded and conducted by a different confidential informant at defendant's residence that corroborated the concerned citizen's account of drug distribution); *United States v. Roberts*, 139 F.3d 895 (4th Cir. 1998) (upholding warrant based on information provided by informants because officer sufficiently corroborated that information); *United States v. Brooks*, No. CRIM. 97-006-H, 1997 WL 327087, at *5 (W.D. Va. June 11, 1997) (upholding warrant where officers had specific and detailed information from four confidential informants that the defendant had previously engaged in a pattern of drug activity involving motel rooms and officers confirmed that pattern by observing the defendant's hotel room on a specific date); *United States v. Lalor*, 996 F.2d 1578, 1581 (4th Cir. 1993) (upholding search warrant for drug activity when one informant stated that s/he had purchased cocaine from the defendant on numerous occasions; two informants described the defendant's alias, address, and area in which he operated; one informant described the defendant's car; both informants corroborated each other; police corroborated what both informants stated; and police independently determined that the defendant had been arrested for drug possession just a few days before the warrant was sought), *cert. denied*, 510 U.S. 983 (1993); *United States v. Miller*, 925 F.2d 695, 696 (4th Cir. 1991) (finding probable cause for warrantless arrest where police substantially corroborated that tip by personally observing the suspect); *United States v. Encarnacion*, 925 F.2d 1457 (4th Cir. 1991) (upholding warrant based on "detailed" and "specific" tip from concerned citizen based on his/her "personal observation:" informant had been in the suspect's motel room, observed two bags of a white rocky substance, and described occupants of the motel room); *United States v. Blackwood*, 913 F.2d 139, 142 (4th Cir. 1990) (upholding search warrant based on anonymous tip that was corroborated by a previously reliable informant's purchase of crack cocaine from the suspect that the officer personally observed).

[22] *See, e.g., United States v. Winters*, 491 F.3d 918, 922 (8th Cir. 2007) (concluding that a "significantly corroborated" tip passed from federal law enforcement officer to state narcotics agents was sufficiently reliable for reasonable suspicion); *United States v. Perez*, 440 F.3d 363, 371 (6th Cir. 2006) (finding reasonable suspicion where original request from one DEA agent to another to surveil a pearl-white Escalade with temporary Kentucky plates was found where the tip indicated it would be, driving in an erratic matter that suggested an attempt to evade surveillance and met up with an unidentified Hispanic female at a gas station); *United States v. Troka*, 987 F.2d 472, 474 (7th Cir. 1993) (finding reasonable suspicion based in part on tip from sister police department since that "police department was a reliable source and because later information provided further corroboration for the tip").

[23] *See, e.g., Reece* Order at 12, 20 (finding "scant evidence" to support probable cause where the supporting affidavit only contained information that "[a]n IP address associated with Defendant either downloaded or attempted to download file content that contained child pornography"); *accord United*

B. The Government's recitation of the case law is misleading.

The Government urges this Court to uphold a search warrant for a family's home—and all electronic devices within it—based on cases that do not support its argument that a vague and conclusory tip, without any corroborating evidence whatsoever, is sufficient. Instead, these cases demonstrate that Courts have upheld warrants only where there was evidence to corroborate the tip and, in the case of child pornography cases, where there was actual evidence that an Internet user at some point possessed specific images of child pornography.

The cases the Government cites for the vague proposition that "probable cause exists to search a home when an IP address linked to that home was used to engage in online child exploitation conduct," Opp'n at 9, all involved affidavits that had evidence of the suspect viewing specific images and videos of child pornography, rather than the vague and conclusory allegation set forth in Paragraph 23.[24]

States v. Falso, 544 F.3d 110, 112 (2d Cir. 2008) (finding that an affidavit alleging that defendant "appear[ed]" to "have gained or attempted to gain" access to a website that distributed child pornography and had been convicted of misdemeanor sexual abuse eighteen years earlier, without more, was insufficient to establish probable cause); *see also United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005) ("Simply the allegation that Coreas logged onto the Candyman website and, by clicking a button, responded affirmatively to a three-sentence invitation ... to join its e-group. The alleged 'proclivities' of collectors of child pornography, on which the district court relied, are only relevant if there is probable cause to believe that Coreas is such a collector. But the only evidence of such . . . is his mere act of responding affirmatively to the invitation to join Candyman. [ ] In the view of this panel, that does not remotely satisfy Fourth Amendment standards.").

[24] *See United States v. Contreras*, 905 F.3d 853, 855-56 (5th Cir. 2018) (affidavit alleged that Internet user with IP address uploaded sexually explicit images of young children to the messaging app Kik); *United States v. Gillman*, 432 F. App'x 513, 514 (6th Cir. 2011) (officers viewed individual share sexually explicit video of a minor to file sharing site); *United States v. Vosburgh*, 602 F.3d 512, 517-18 (3d Cir. 2010) (individual clicked, three times in a two-minute time period, on "dummy link" set up by the FBI entitled "4yo_suck" on a website dedicated exclusively to child pornography); *United States v. Richardson*, 607 F.3d 357, 360-61 (4th Cir. 2010) (law enforcement traced multiple sent emails containing child pornography images to the same individual over a fifteen-month timespan); *United States v. Perez*, 484 F.3d 735, 738 (5th Cir. 2007) (affidavit alleged that user with IP address had showed individual "images of young children engaged in sexual acts" over webcam).

The cases the Government cites for the proposition that "the unique characteristics of child pornography sites on Tor can be used to draw favorable inferences in support of probable cause," Opp'n at 9-10, are also distinguishable and do not support the razor-thin basis for probable cause proffered here.[25] In *United States v. Bosyk*, the Fourth Circuit found probable cause where the FBI described a posting on a Tor Onion Service website with a URL with numerous thumbnail images depicting man sexually molesting a female toddler, which was unmistakably child pornography, and records subpoenaed from a file-sharing site showed the defendant had viewed and clicked on the URL for the file-sharing site to download child pornography.[26] The Government's attempt to minimize the facts of *Bosyk*, and distinguish it from those here, misses the mark.[27] The facts in *Bosyk* are far more incriminating—and do far

---

[25] *See United States v. DeFoggi*, 839 F.3d 701, 707 (8th Cir. 2016) (website in question was named "PedoBook," a name that clearly indicated child pornography would be present, unlike "Hurt Meh." Further, the FBI conducted extensive investigation in that case that it did not here, which revealed that the user posted on multiple child pornography websites, accessed specific filenames of child pornography, sent private messages, and eventually led to the FBI having a phone conversation with the user, all before the affidavit was issued); *see also United States v. Taylor*, 935 F.3d 1279, 1282 (11th Cir. 2019), *as corrected* (Sept. 4, 2019), *cert. denied*, 140 S. Ct. 1548 (2020) (website at issue was Playpen, which had images that made it clear that it contained child pornography) ("Tor has plenty of legitimate uses—think military and law-enforcement officers carrying out investigations, journalists seeking to maintain anonymity, and ordinary citizens researching embarrassing topics."); *United States v. Tagg*, 886 F.3d 579, 587 (6th Cir. 2018) (listing unlikely accidental stumbling onto Playpen amongst multiple factors for probable cause that are not present here, including that defendant spent over five hours on the website and clicked on over 160 hyperlinks that "blatantly" advertised child pornography).

[26] 933 F.3d 319, 322 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 1124 (2020).

[27] Opp'n at 10, 13. Puzzlingly, the Government attempts to argue that in *Bosyk*, "[u]nlike here," there was no allegation that the user was on Tor before his IP address accessed the link posted on Bulletin Board A—a Tor Onion Service website—nor an allegation that the user actually viewed child sexual abuse material prior to or after accessing the link. *Id.* That is incorrect, and the opposite of what the Government argued in *Bosyk*. In litigating the suppression issue in *Bosyk*, the Government asserted that the facts in the affidavit "establish[ed] a fair probability that the link was accessed through Bulletin Board A," "there was no reason for the [affiant] agent to believe that the link was available anywhere other than on Bulletin Board A," and "it [wa]s unlikely the [link] was accessed somewhere else given the close proximity in time between the posting at Bulletin Board A and attempt to download its child pornographic content." Gov't Opp'n to Defendant's Motion to Suppress in *United States v. Nikolai Bosyk,* 17-CR-302 (E.D. Va. 2018) ("*Bosyk* Opp'n") at 8-9. Here, as in *Bosyk*, the Affidavit alleges [redacted]

more to establish probable cause—than those present here. In *Bosyk*, the link in question was posted on Bulletin Board A, in the "Pre-teen Hardcore section," with graphic descriptions of four videos and three sets of 20 video thumbnail images showing "juvenile females engaged in sexual acts."[28] The very same day the post was published, Mr. Bosyk visited the link to those videos.[29] Here, unlike in *Bosyk*, the [redacted]. Here, unlike in *Bosyk*, the Affidavit failed to provide *any information* about [redacted] (whereas the IP address in *Bosyk* was linked to videos that included "an adult male using his fingers to spread the vagina of a female who appear[ed] to be a toddler").[30] And the name of the website here [redacted], unlike the "Preteen Hardcore" message board with its explicit descriptions in *Bosyk*. There was accordingly far more evidence supporting probable cause in *Bosyk* than there was here.

C. This Court should not break new ground.

This Court should not find probable cause where no other Court has done so. Upholding this search warrant would allow law enforcement to accept a single uncorroborated and vague allegation to justify searching all of a family home. Doing so would give a green light to future warrants that also lacked any independent law enforcement investigative work or corroboration.

[28] *Bosyk*, 933 F.3d at 323.

[29] *Id.*

[30] *Bosyk* Opp'n at 6.

II. A warrant cannot be based on misleading statements and omissions: had the Special Agent told the Magistrate what he well knew—that there was no actual evidence that this Internet viewed illegal content—and accurately explained [redacted], the Magistrate would not have issued the warrant.

A. The Affidavit misled the Magistrate about the true state of the Government's evidence: contrary to what the Affidavit suggested, the Special Agent knew there was no actual evidence that this Internet user ever viewed or downloaded illegal content.

In its Opposition, the Government presents a caricature of Mr. Sanders's argument on the misleading nature of paragraph 23. The issue is not whether the [redacted] or the Special Agent "lied," Opp'n at 17, and the Government's obvious attempt to inflame the Court by mischaracterizing Mr. Sanders's position should be rejected. Instead, the issue is whether the unqualified reiteration of [redacted] misled the Magistrate into believing that there was actual evidence the Internet user [redacted] *i.e.*, viewed or downloaded, child pornography, when the Special Agent did not believe that to be the case at the time he submitted the Affidavit. And on that issue, the evidence is more than sufficient to entitle Mr. Sanders to a *Franks* hearing.

A comparison of [redacted] conclusively demonstrates the misleading nature of the statement that the Internet user [redacted] Affidavit, ¶ 23. In making that statement, Paragraph 23 clearly suggested to the Magistrate the existence of evidence that the Internet user had ([redacted] Indeed, at no point has the Government disagreed with that characterization of Paragraph 23. Furthermore, it is Paragraph 23—when combined with the Government's total failure to ever inform the Court of *what the Special Agent actually understood* (despite submitting a Declaration from the Special Agent himself)—that is responsible for this Court mistakenly

concluding in its Memorandum Opinion that it is "obvious" that Paragraph 23 "*describes an internet user's activity on a website*." Mem. Op. (ECF No. 73) at 10 (emphasis added).

To see how the Affidavit led both the Magistrate Judge and this Court to an erroneous conclusion regarding the Government's evidence, one need look no further than [redacted] Affidavit at 15 (emphasis added).

[redacted] the Special Agent knew that the evidence did not support the allegation [redacted]. [redacted] states in full:

> [redacted].

Id., ¶ 29 (emphasis added). Finally, in Paragraph 30, the Special Agent summarizes [redacted] *Id.*, ¶ 30 (emphasis added).

The Special Agent would not have described [redacted]—if he believed there was evidence of the Internet user viewing and/or downloading child pornography.

Nor would the Special Agent have written anything close to [redacted] And finally, if the Special Agent was aware of actual evidence that the Internet user viewed or downloaded child pornography, then there is no possibility he would have premised his argument for probable cause on the proposition that [redacted] *Id.*, ¶ 30.

If the defense is wrong about the Special Agent's state of mind—and notably the Government has at no time stated directly that it is—there is no reason to advance the dubious argument that probable cause exists to search the home of anyone who [redacted], as the Special Agent did in the Affidavit, *see id.*, ¶¶ 29-20, and as the Government does on pages 19-20 of its Opposition. If the FBI wanted a warrant, then this visiting-the-website theory of probable cause is the candid, non-misleading case it needed to—but did not—present to the Magistrate, even though it would have clearly failed on its merits.[31] Instead of presenting this truthful case for a warrant based on the actual state of the evidence, however, the Special Agent misled the Magistrate into believing what the Government has likewise misled this Court into believing: that Paragraph 23 was "*describ[ing] an internet user's activity on a*

[31] *Cf. United States v. Richardson*, 607 F.3d 357 (4th Cir. 2010) (finding probable cause where investigation linked defendant's email accounts, which he used to distribute child pornography, to the address where the warrant was executed); *United States v. Bynum*, 604 F.3d 161 (4th Cir. 2010) (finding probable cause where someone with a particular screen name at address where warrant was executed had uploaded suspected child pornography to the Internet); *United States v. Goodwin*, 854 F.2d 33 (4th Cir. 1988) (finding probable cause for anticipatory search warrant when defendant ordered child pornography and investigation verified that materials would be delivered to address where warrant was executed); *United States v. Bailey*, 272 F. Supp. 2d 822, 824 (D. Neb. 2003) (finding probable cause where someone using a particular e-mail address knowingly subscribed to a specialized Internet site that distributed child pornography).

website," Mem, Op. at 10 (emphasis added), when both the Special Agent (then) and the Government (now) well know that was not the case.

The contrary proposition—that the Special Agent knew of evidence of the Internet user accessing or downloading child pornography, but chose instead to focus repeatedly [redacted]—makes no sense; indeed, it does not pass the straight-face test. And if more was needed to establish Mr. Sanders's right to a *Franks* hearing (which it is not), the Special Agent's own [redacted] FD-1057, attached to Motion to Suppress No. 1 (ECF No. 81) as Ex. 4. Indeed, though the Special Agent noted that the Internet user [redacted] Nor did the Special Agent suggest otherwise in his Declaration submitted to this Court. Attached as Ex. 2 to Gov't Brief (ECF No. 53). The Special Agent has never suggested such evidence existed—[redacted]—because he knew it did not.

Indeed, the Government essentially concedes that the Special Agent knew there was no evidence of the Internet user viewing or downloading child pornography when it tellingly (but unconvincingly) argues that [redacted]. *See* Gov't Opp'n at 19 ("In fact, as [the defense] points out in [its] motion, the Affidavit actually states that [redacted] and the magistrate judge still issued the warrant."). Not so. Accurately stating

the Government's evidence [redacted] did not un-ring the bell of Paragraph 23. To the contrary, the Special Agent (then) and the Government (now) are trying to have it both ways, by professing belief in Paragraph 23 while simultaneously making the non-misleading case for probable cause based on the actual state of the evidence.[32] The obvious reality is that the Special Agent understood there was no actual evidence that the Internet user viewed or downloaded child pornography, and that is why [redacted] and nothing more.

B. The Affidavit misled the Magistrate about [redacted] and evidence of the Internet user's intent.

The Affidavit represented that [redacted] the Tor network is easy to use; it is not primarily designed or used for illegal purposes; there are many legitimate reasons for people to

[32] Opp'n at 19 ("assuming that the defendant is somehow correct that [redacted] . . ."); *see also id*. at 20 ("[E]ven if the defendant's unsupported theory about what the [redacted] meant is correct, and even if his speculation that SA [redacted] shared his view of the meaning of the tip is true . . . ").

access the Tor network and use the Tor Browser; the Tor Browser is easy to download and use and requires the same steps as downloading and using any non-default browser, like Google Chrome or Mozilla Firefox; [redacted] was not exclusively dedicated to child pornography but contained a mix of legal and illegal content; an Internet user easily could have encountered [redacted] using a search engine or clicking on a link, without intending or attempting to view child pornography;[33] this Internet user was only alleged to have [redacted] and there was no evidence that the Internet user had any of the characteristics common to individuals with a sexual interest in children or visual depictions in children.

Contrary to what the Government asserted,[34] Internet users can easily use search engines such as DuckDuckGo or Torch to browse Tor Onion Service websites, and this is a more common way to browse the Internet, including Tor Onion Service websites, than by memorizing 16-or-56 character web addresses. Assuming *arguendo* that the Internet user ever navigated to [redacted], for example, by clicking on search engine results or a hyperlink, there was no evidence that this Internet user had reason to know the nature of [redacted] or that child pornography was what the Internet user was looking for given a [redacted] with legal and illegal content.

A [redacted]—does not demonstrate an interest in viewing child pornography.[35]

---

[33] *See* Declaration of Seth Schoen, attached to Motion to Suppress No. 3 (ECF No. 83) as Ex. 7.

[34] Opp'n at 4-5, 10 n.4, 27-28.

[35] In *United States v. Tagg*, 886 F.3d 579, 582 (6th Cir. 2018), which the Government cited favorably, the FBI had "digital evidence . . . showing that Tagg had spent over five hours browsing a website ("Playpen") that obviously contained child pornography." A visit for [redacted] to a website containing both illegal and legal material does not evidence the intent that a five-hour visit to an exclusively child pornography website does.

Including detailed information about characteristics of people with a sexual interest in children or visual depictions in children, without any actual evidence that the Internet user shared such characteristics, "can lead to recklessly misleading results," particularly in the "absence of clarifying information that either tailor [these characteristics to the Internet user] or acknowledged the lack of such connections:" a Magistrate may incorrectly "infer that Defendant may have fit the profile of a 'collector' of child pornography"[36] where there is no evidence to show that the Internet user fit such a profile. Had the Special Agent disclosed the above information to the Magistrate, the Magistrate would not have found a substantial basis to believe that the Internet user had intended or attempted to view child pornography.[37]

C. The Affidavit misled the Magistrate about the subject premises and places where evidence of wrongdoing could be found.

The Affidavit strongly suggested that evidence of child pornography would be found in the Sanders's home more than eight months later. Child pornography cases rejecting challenges for staleness relied on affidavits that alleged that the accused either distributed child pornography or collected child pornography and were based on the view "that *collectors and distributors* of child pornography value their sexually explicit materials highly, rarely if ever dispose of such material, and store it for long periods in a secure place, typically in their homes."[38]

---

[36] *Reece* Order at 20-21.

[37] *Cf. United States v. Shields*, No. 4:CR-01-0384, 2004 WL 832937, at *7 (M.D. Pa. Apr. 14, 2004), *aff'd*, 458 F.3d 269 (3d Cir. 2006) (finding probable cause where defendant voluntarily subscribed to and joined two websites whose purpose was to share child pornography); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004) (finding probable cause where the defendant paid to join a group called Candyman where sole purpose was to receive and distribute child pornography, the defendant registered screennames that reflected an interest in child pornography, and the defendant did not cancel his paid subscription); *United States v. Hutto*, 84 F. App'x 6, 8 (10th Cir. 2003) (finding probable cause where the defendant paid to join a group where images of child pornography were available to all members).

[38] *United States v. Richardson*, 607 F.3d 357, 370 (4th Cir. 2010) (quotation marks omitted) (emphasis added).

Given the lack of evidence that the Internet user had any interest in collecting child pornography and the heightened protections of the Tor Browser, the Special Agent should have disclosed to the Magistrate that there was no reason to think that any evidence of an Internet user's purported activity on Tor, let alone any illegal activity, would be present in the Sanders's family home more than eight months after [redacted].[39] As a result, the Magistrate was misled into issuing an overbroad warrant that authorized a sweeping search of every room and person in a family home, and through the electronic devices of all three family members—none of whom were an identified suspect—without any attempt to limit its scope.[40]

D. The Affidavit misled the Magistrate about how the Internet user was identified—which goes directly to the foreign officers' and agent's credibility.

Contrary to what the Government claimed in its Opposition, defense experts Dr. Richard Clayton and Dr. Matthew Miller have demonstrated that there is no method possible in practice that the [redacted] could have used to identify accurately an Internet user's IP address based on [redacted] Nor does the Government explain how, given that the [redacted], the Special Agent did not know (or should not have known) that the [redacted]

[39] *See, e.g., United States v. Doyle*, 650 F.3d 460, 476 (4th Cir. 2011) (holding warrant invalid and good faith exception inapplicable where there was no evidence that the material described actually constituted child pornography and nothing indicated when or if child pornography allegedly existed in the defendant's home); *Cf. United States v. Davis*, 313 F. App'x 672, 2009 WL 289998, at *1 (4th Cir. Feb. 27, 2009) (recognizing circuits that have found people who *collect* child pornography keep their contraband for a long time, and that information that is a year old is not stale in such cases) (emphasis added).

[40] *See, e.g., United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1177 (9th Cir. 2010) (recognizing the dangers of over-searching when conducting electronic searches "calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.")

The sworn statements from three defense experts have placed the [redacted]'s and the Special Agent's credibility squarely at issue and are more than sufficient to warrant a *Franks* hearing.[41]

E. Individually and taken together, these misleading statements and omissions were material.

The Affidavit's misleading statements and omissions were essential to the Magistrate finding probable cause.[42] The exclusionary rule is appropriate here because the Affidavit demonstrates "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, [and] the deterrent value of exclusion is strong and tends to outweigh the resulting costs."[43]

III. The good faith exception does not apply.

Suppression is appropriate here because the good faith exception does not apply. Reliance on an affidavit based on little more than an IP address and a conclusory, uncorroborated hearsay allegation of possible criminal conduct has never been enough to search a family's home for evidence of child pornography. These defects were plain from the face of the Affidavit and should have been evident to the FBI, the Special Agent, and the Magistrate. "Where, as here, the executing officer is also the affiant—and the same officer who misled the issuing judge—the good faith exception to the exclusionary rule cannot apply, because it cannot be said that the executing officer reasonably relied on the search warrant."[44]

---

[41] To the extent Mr. Sanders has not shown with one hundred percent certainty what the [redacted] did here, that is only because he has been unfairly denied further discovery required to show conclusively that the [redacted] If the [redacted] to interfere with the Internet user's computer, the only technique the [redacted] could have used would not have been able to identify accurately the Internet user in this case and would not support the FBI's assertion that the Internet user ever [redacted]. Mr. Sanders incorporates by references the arguments he made in his Renewed Motion to Compel and Reply to the Government's Opposition to his Renewed Motion to Compel.

[42] *United States v. Doyle*, F.3d 460, 469 (4th Cir. 2011).

[43] *United States v. Stephens*, 764 F.3d 327, 336 (4th Cir. 2014) (quotation marks and citations omitted).

[44] *Reece* Order at 25.

CONCLUSION

Because this warrant was based entirely on a vague, conclusory, and uncorroborated tip, this Court should not break new legal ground by finding probable cause on less than any other Court. Furthermore, the Special Agent knew that what the [redacted] meant to communicate in their tip was insufficient for probable cause—[redacted] make this fact crystal-clear. And the Special Agent knowingly and recklessly misled the Magistrate with other misleading statements and omissions on matters fundamental to probable cause. Under these circumstances, the good faith exception does not apply, and all evidence derived from the illegal search of the Sanders's family home must be suppressed.

Respectfully submitted,

/s/ Jonathan Jeffress

Jonathan Jeffress (#42884)
Emily Voshell (#92997)
Jade Chong-Smith (admitted *pro hac vice*)
KaiserDillon PLLC
1099 Fourteenth St., N.W.; 8th Floor—West
Washington, D.C. 20005
Telephone: (202) 683-6150
Facsimile: (202) 280-1034
Email: jjeffress@kaiserdillon.com
Email: evoshell@kaiserdillon.com
Email: jchong-smith@kaiserdillon.com

Counsel for Defendant Zackary Ellis Sanders

CERTIFICATE OF SERVICE

I hereby certify that on this 10th day of September 2020, the foregoing was served electronically on the counsel of record through the U.S. District Court for the Eastern District of Virginia Electronic Document Filing System (ECF) and the document is available on the ECF system.

/s/ Jonathan Jeffress
Jonathan Jeffress